Requirement ID: [SRS-4-206]

The IEG-C Low Domain Firewall component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the low domain; one for the network connection to the Low Domain Network Switch; and, one for the network connection to the Management Domain Network Switch).

Requirement ID: [SRS-4-207]

The IEG-C Low Domain Firewall component network interfaces to the low domain SHALL be 1000-BaseSX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-208]

The IEG-C Low Domain Firewall component network interfaces to the Low Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

4.3 Network Switch

4.3.1 General

Requirement ID: [SRS-4-67]

The IEG-C Network Switch components (High Domain, Low Domain and Management) SHALL be selected from the following list of products:

- Dell Networking N1124T Switch
- Dell Networking S3048 Switch
- Dell Networking S3124F Switch
- Dell Networking S3148P Switch

Detailed descriptions of these component options are provided in Appendix D.

Requirement ID: [SRS-4-209]

The selected IEG-C Network Switch components SHALL include compatible rack mount kits and power cords.

Requirement ID: [SRS-4-68]

The IEG-C Network Switch components SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.3.2 Data Exchange Services

Requirement ID: [SRS-4-69]

The IEG-C Network Switch components SHALL enable the Data Exchange Services as specified in Table 4 (for that component).

4.3.3 Element Management Services

Requirement ID: [SRS-4-70]

The IEG-C High Domain Network Switch and Low Domain Network Switch components SHALL be enabled and configured with the capability for being managed as specified in Section 9.

4.3.4 Hardware and Software

Requirement ID: [SRS-4-71]

The IEG-C High Domain Switch component SHALL be configured to have at least five network interfaces (NICs: one for the network connection to the High Domain Firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-72]

The IEG-C High Domain Network Switch component network interface to the high domain firewall SHALL be 1000BASE-SX gigabit Ethernet interface.

Requirement ID: [SRS-4-73]

The IEG-C High Domain Network Switch component network interfaces to the Mail Guard, Web Guard, server component and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-74]

The IEG-C Low Domain Switch components SHALL be configured to have at least five network interfaces (NICs: one for the network connection to the Low Domain firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-75]

The IEG-C Low Domain Network Switch component network interface to the Low Domain Firewall SHALL be 1000BASE-SX gigabit Ethernet interface.

Requirement ID: [SRS-4-76]

The IEG-C Low Doman Network Switch component network interfaces to the Mail Guard, Web Guard, server component and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-77]

The IEG-C Management Domain Switch component SHALL be configured to have at least seven network interfaces (NICs: one for the network connection to the High Domain Firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component;

one for the network connection to the High Domain Network Switch, one for the network connections to the Low Domain Network Switch and one for the network connection to the Low Domain Firewall).

Requirement ID: [SRS-4-78]

The IEG-C Management Domain Network Switch component network interface to the Firewall SHALL be a 1GbE interface.

Requirement ID: [SRS-4-79]

The IEG-C Management Domain Network Switch component network interfaces to the Mail Guard, Web Guard, server component, High Domain Switch and Low Domain Switches SHALL be 1GbE interfaces.

4.4 Web Proxy

4.4.1 General

Requirement ID: [SRS-4-81]

The IEG-C Web Proxy component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.4.2 Data Exchange Services

Requirement ID: [SRS-4-82]

The IEG-C Web Proxy component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

4.4.3 Protection Services

Requirement ID: [SRS-4-83]

The IEG-C Web Proxy component SHALL enable the capability to perform cryptographic operations and key management to support interception of Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.

Requirement ID: [SRS-4-229]

The IEG-C Web Proxy component SHALL support the use Simple Certificate Enrolment Protocol (SCEP) [IETF RFC 8894, 2020] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.

Requirement ID: [SRS-4-230]

The IEG-C Web Proxy component SHOULD support the use of Enrolment over Secure Transport (EST) [IETF RFC 7030, 2013] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.

Requirement ID: [SRS-4-84]

The IEG-C Web Proxy component SHALL be configured to conform to the INFOSEC CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-4-85]

The IEG-C Web Proxy component SHALL be configured to conform to the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms [NAC AC/322-D/0047-REV2 (INV), 2009].

Requirement ID: [SRS-4-86]

The IEG-C Web Proxy component provided cryptographic mechanism SHALL be configured based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].

Requirement ID: [SRS-4-87]

The IEG-C Web Proxy component SHALL use a malware/virus scanner that is included in the NATO Information Assurance Product Catalogue (NIAPC) to check web content for malicious content.

4.4.4 Protection Policy Enforcement Services

Requirement ID: [SRS-4-89]

The IEG-C Web Proxy components SHALL enable the capability to be configured as a reverse web proxy from the high domain to the low domain.

Requirement ID: [SRS-4-90]

The IEG-C Web Proxy component SHALL be configurable to support the enforcement of the following IEG-C SOA Platform IFPs (see Section 3.4.4):

- IEG-C_IFP_SOA_HL - SOA Platform Services High to Low IFP; and,
- IEG-C_IFP_SOA_LH - SOA Platform Services Low to High IFP.

Requirement ID: [SRS-4-91]

The IEG-C Web Proxy component SHALL be configurable to support the enforcement of the following IEG-C SOA Platform CIP (see Section 3.4.5):

- IEG-C_CIP_SOA_LH - SOA Platform Services Low to High CIP.

Requirement ID: [SRS-4-92]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL IFP in order to guard HTTP application-level web browsing requests from the high domain to the low domain.

Requirement ID: [SRS-4-93]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_LH IFP in order to guard HTTP application-level web browsing responses from the low domain to the high domain.

Requirement ID: [SRS-4-94]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and IEG-C_IFP_SOA_LH IFPs to verify that the HTTP request (from the high domain to the low domain) and HTTP response (from the low domain to the high domain) can be released by checking high domain web client access control rules against white or black lists (assuring only authorised high domain clients (or users) have access to the low domain web content).

Requirement ID: [SRS-4-95]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and IEG-C_IFP_SOA_LH IFPs to verify that the HTTP request (from the high domain to the low domain) and HTTP response (from the low domain to the high domain) can be released by checking low domain web server access control rules against white or black lists (assuring only authorised low domain web servers are published and made accessible for high domain clients).

Requirement ID: [SRS-4-96]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_LH IFP to enforce the IEG-C_CIP_SOA_LH CIP.

Requirement ID: [SRS-4-97]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_CIP_SOA_LH CIP to verify that all HTTP responses from the low domain to the high domain (to HTTP requests from the high domain to the low domain) do not contain any disallowed attachment types by checking against a white list or black list of attachment types.

Requirement ID: [SRS-4-98]

The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_CIP_SOA_LH CIP to verify that all HTTP responses from the low domain to the high domain (to HTTP requests from the high domain to the low domain) contain no malicious content.

Requirement ID: [SRS-4-231]

The IEG-C Web Proxy component SHALL ensure HTTP request or response does not contain any of the configured words/phrases.

Requirement ID: [SRS-4-232]

The IEG-C Web Proxy component SHALL inspect each of the HTTP request or response, including any attachments, for occurrences of any of the configured words/phrases.

Requirement ID: [SRS-4-233]

The IEG-C Web Proxy component SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when searching for each of the configured words/phrases in the http request or response and any attachments.

Requirement ID: [SRS-4-99]

The IEG-C Web Proxy component SHALL enforce the IEG-C SOA Platform IFPs and SOA Platform CIP configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.

4.4.5 Element Management Services

Requirement ID: [SRS-4-100]

The IEG-C Web Proxy component SHALL be enabled and configured with the capability for being managed as specified in Section 9.

4.4.6 Hardware and Software

Requirement ID: [SRS-4-101]

The IEG-C Web Proxy component SHALL be an appliance, or deployed on a physical server.

Requirement ID: [SRS-4-103]

The IEG-C Web Proxy component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connection to the Low Domain Switches; and, one for the network connection to the Management Domain Switch).

4.5 RDP Proxy

4.5.1 General

Requirement ID: [SRS-4-105]

The IEG-C RDP Proxy component SHALL be the Microsoft Windows Server 2016 (or later versions that are listed on the Approved Fielded Product List for the High Side) with the Remote Desktop Services server role.

Requirement ID: [SRS-4-106]

The IEG-C RDP Proxy component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.5.2 Data Exchange Services

Requirement ID: [SRS-4-107]

The IEG-C RDP Proxy component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

Requirement ID: [SRS-4-210]

Only configured users SHALL be allowed to connect to the RDP Proxy.

Requirement ID: [SRS-4-211]

Users SHALL be required to authenticate to the RDP Proxy in accordance with [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-4-212]

Authenticated users SHALL be required to authenticate to the RDP Proxy in accordance with [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-4-213]

An authenticated user SHALL only be able to connect to a configured set of network resources.

Requirement ID: [SRS-4-106]

Local client devices SHALL NOT be accessible on the remote desktop session.

4.5.3 Element Management Services

Requirement ID: [SRS-4-107]

The IEG-C RDP Proxy component SHALL be enabled and configured with the capability for being managed as specified in Section 9.

Requirement ID: [SRS-4-108]

The IEG-C RDP Proxy component SHALL generate an SSL Certificate Signing Request (CSR) to be signed by the appropriate E-NPKI Registration Authority (RA).

4.5.4 Hardware and Software

Requirement ID: [SRS-4-109]

The IEG-C RDP Proxy component SHALL be deployed on a physical server.

Requirement ID: [SRS-4-110]

The IEG-C RDP Proxy component server SHALL support (as a minimum) the Microsoft Windows Server 2016 R2 (or later versions that are listed on the Approved Fielded Product List for the High Side) 64-bit edition operating system.

Requirement ID: [SRS-4-111]

The IEG-C RDP Proxy component server SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

4.6 Web Guard

4.6.1 General

Requirement ID: [SRS-4-113]

The IEG-C Web Guard component SHALL comply with the functional requirements specified in Section 6.

Requirement ID: [SRS-4-114]

The IEG-C Web Guard component SHALL comply with the non-functional requirements specified in Section 5.3.

Requirement ID: [SRS-4-115]

The IEG-C Web Guard component SHALL comply with the security functional requirements specified in Section 6.8.

Requirement ID: [SRS-4-116]

The IEG-C Web Guard component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

Requirement ID: [SRS-4-118]

It SHALL be possible to enforce a separate 'WG security policy' (see section 6.2.1) per service/application mediated by the Web Guard.

4.6.2 Data Exchange Services

Requirement ID: [SRS-4-119]

The IEG-C Web Guard component SHALL enable the capability to support only those Data Exchange Services as listed in Table 4 (for that component) and specified in Section 6.4.

4.6.3 Protection Services

Requirement ID: [SRS-4-120]

The IEG-C Web Guard component Protection Services SHALL comply with the requirements specified in Section 6.6.

4.6.4 Protection Policy Enforcement Services

Requirement ID: [SRS-4-121]

The IEG-C Web Guard component Protection Policy Enforcement Services SHALL comply with the requirements specified in Section 6.5.

4.6.5 Element Management Services

Requirement ID: [SRS-4-122]

The IEG-C Web Guard component Element Management Services SHALL comply with the requirements specified in Section 6.7.

4.6.6 Hardware and Software

Requirement ID: [SRS-4-123]

The IEG-C Web Guard component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connection to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-124]

The IEG-C Web Guard component network interfaces to the High Domain Switch, Low Domain Switches and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

4.7 Mail Guard

4.7.1 General

Requirement ID: [SRS-4-126]

The IEG-C Mail Guard component SHALL be synchronised to the IEG-C Firewall component NTP source.

4.7.2 Data Exchange Services

Requirement ID: [SRS-4-127]

The IEG-C Mail Guard component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).

4.7.3 Protection Services

Requirement ID: [SRS-4-128]

The IEG-C Mail Guard component SHALL use a malware/virus scanner that is included in the NATO Information Assurance Product Catalogue (NIAPC) to check email messages for malicious content.

Requirement ID: [SRS-4-129]

The IEG-C Mail Guard component SHALL enable the capability to configure the Content Inspection Services that will enforce the IEG-C Business Support and COI CIPs (refer to Section 4.7.4) depending on the information exchange requirements and the content inspection policy to be enforced for the CIS interconnection.

Requirement ID: [SRS-4-130]

The IEG-C Mail Guard component SHALL enable the capability to perform cryptographic operations and key management to support the validation of cryptographic bindings according to NISP Cryptographic Artefact Binding Profiles [ADatP-34(I), NISP Version 10, 2017].

Requirement ID: [SRS-4-131]

The IEG-C Mail Guard component SHALL be configured to conform to the INFOSEC CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].

Requirement ID: [SRS-4-132]

The IEG-C Mail Guard component SHALL be configured to conform to the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms [NAC AC/322-D/0047-REV2 (INV), 2009].

Requirement ID: [SRS-4-133]

The IEG-C Mail Guard component provided cryptographic mechanism SHALL be configured based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].

4.7.4 Protection Policy Enforcement Services

Requirement ID: [SRS-4-134]

The IEG-C Mail Guard component SHALL be configurable to support the enforcement of the following IEG-C Business Support IFPs (see Section 3.4.4):

- MG_IFP_BS_HL - Business Support Services High to Low IFP; and,
- MG_IFP_BS_LH - Business Support Services Low to High IFP.

Requirement ID: [SRS-4-135]

The IEG-C Mail Guard component SHALL be configurable to support the enforcement of the following IEG-C Business Support CIPs (see Section 3.4.5):

- MG_CIP_BS_HL - Business Support Services High to Low CIP; and,
- MG_CIP_BS_LH - Business Support Services Low to High CIP.

Requirement ID: [SRS-4-136]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL IFP in order to guard SMTP application-level traffic from the high domain to the low domain.

Requirement ID: [SRS-4-137]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_LH IFP in order to guard SMTP application-level traffic from the low domain to the high domain.

Requirement ID: [SRS-4-138]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL and MG_IFP_BS_LH IFPs to verify that the email message can be forwarded between the high and low domain by checking originator access control rules against white or black lists.

Requirement ID: [SRS-4-139]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL and MG_IFP_BS_LH IFPs to verify that the email message can be transferred between the high and low domain by checking recipient access control rules against white or black lists.

Requirement ID: [SRS-4-140]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL IFP to enforce the MG_CIP_BS_HL CIP.

Requirement ID: [SRS-4-141]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL CIP to verify that all email messages to be released from the high domain to the low domain contain a security label that conforms to the access control rules to be enforced for the CIS interconnection.

Requirement ID: [SRS-4-142]

The IEG-C Mail Guard component SHALL enable the capability to select that the security label format is the STANAG 4774 confidentiality label XML format.

Requirement ID: [SRS-4-143]

The IEG-C Mail Guard component SHALL enable the capability to select that the STANAG 4774 confidentiality label is bound to the email message as specified in STANAG 4778 and NATO Interoperability Standards and Profiles (NISP) SMTP Binding Profile.

Requirement ID: [SRS-4-144]

The IEG-C Mail Guard component SHALL enable the capability to select that the STANAG 4774 confidentiality label is cryptographically bound to the email message as specified in NATO Interoperability Standards and Profiles (NISP) Cryptographic Artefact Binding Profiles.

Requirement ID: [SRS-4-145]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL CIP to verify that all email messages to be released from the high domain to the low domain do not contain unauthorised information, such as 'dirty words'.

Requirement ID: [SRS-4-146]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_LH IFP to enforce the MG_CIP_BS_LH CIP.

Requirement ID: [SRS-4-147]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL and MG_CIP_BS_HL CIPs to verify that all email messages to be forwarded between the high domain and the low domain do not contain any disallowed attachment types by checking against a white list or black list of attachment types.

Requirement ID: [SRS-4-148]

The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_LH CIP to verify that all email messages (including email message header, body and allowed body parts) are well-formed, valid and contain no malicious content.

Requirement ID: [SRS-4-149]

Depending on the information exchange requirements the IEG-C SHALL be configurable to support the enforcement of the following IEG-C COI CIPs (see Section 3.4.5):

- IEG-C_CIP_COI-ES_HL - COI-Enabling Services High to Low CIP;
- IEG-C_CIP_COI-ES_LH - COI-Enabling Services Low to High CIP;
- IEG-C_CIP_COI_HL - COI-Specific Services High to Low CIP; and
- IEG-C_CIP_COI_LH - COI-Specific Services Low to High CIP.

Requirement ID: [SRS-4-150]

The IEG-C Mail Guard component SHALL enable the capability to configure the IEG-C_CIP_COI-ES_HL and IEG-C_CIP_COI_HL CIPs to verify that attachments contained in email messages to be released from the high domain to the low domain do not contain unauthorised information, such as 'dirty words', including classification markings.

Requirement ID: [SRS-4-151]

The IEG-C Mail Guard component SHALL enable the capability to configure the IEG-C_CIP_COI-ES_LH and IEG-C_CIP_COI_LH CIPs to verify that attachments contained in email messages are well-formed, valid and contain no malicious content.

Requirement ID: [SRS-4-152]

The IEG-C Mail Guard component SHALL enforce the IEG-C Business Support IFPs, Business Support CIPs and COI CIPs configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.

4.7.5 Element Management Services

Requirement ID: [SRS-4-153]

The IEG-C Mail Guard component SHALL be enabled and configured with the capability for being managed as specified in Section 9.

4.7.6 Hardware and Software

Requirement ID: [SRS-4-154]

The IEG-C Mail Guard component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-155]

The IEG-C Mail Guard component network interfaces to the High Domain Switch, Low Domain Switches and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

4.8 Management Workstation

The management workstation is deployed in the management domain and is used to manage multiple IEG-Cs.

Requirement ID: [SRS-4-214]

The IEG-C management workstation component SHALL be the Dell Optiplex 5070 SFF.

Requirement ID: [SRS-4-215]

The IEG-C management workstation monitor SHALL be the Dell P2419H Monitor.

Requirement ID: [SRS-4-216]

The IEG-C management workstation keyboard SHALL be the Dell KB216 Multimedia Keyboard.

Requirement ID: [SRS-4-217]

The IEG-C management workstation mouse SHALL be the Dell 6 Button Laser Mouse.

A detailed description of these components is provided in Appendix D.

4.9 Supporting Components

Supporting components of the IEG-C do not directly support the operational requirements provided by the IEG-C but are required for the overall composition of an IEG-C.

4.9.1 Server

Requirement ID: [SRS-4-156]

The IEG-C server SHALL be integrated with either

- HPE OneView and HPE Integrated Lights-Out (iLO); or
- Dell EMC OpenManage Enterprise and Dell Integrated Dell Remote Access Controller (iDRAC)

Requirement ID: [SRS-4-158]

The IEG-C server component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).

Requirement ID: [SRS-4-159]

The IEG-C server component network interfaces to the High Domain Switch, Low Domain Switch and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.

Requirement ID: [SRS-4-160]

The IEG-C server component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.

4.9.2 Hypervisor

Requirement ID: [SRS-4-218]

Any IEG-C component MAY host a Type 1 Hypervisor, provided that the overall IEG-C system design meets the requirements of “Technical and Implementation Directive for CIS Security” [NAC AC/322-D/0048-REV3, 2019] (see SRS-4-4).

Requirement ID: [SRS-4-219]

The Type 1 Hypervisor for the server and the management workstation, if used, SHALL be the VMWare ESXi hypervisor.

4.9.3 Keyboard, Video and Mouse (KVM)

All management of the IEG-C components shall be performed remotely, therefore there is no requirement for a rack-based keyboard, monitor, mouse or KVM switch. However, future deployed versions of the IEG-C, that may be exercised as options, will require local management as a main or a backup solution, so there needs to be provision for the use of a rack that will allow the addition of rack-based keyboard, monitor, mouse or KVM switch.

4.9.4 Rack

Requirement ID: [SRS-4-165]

The IEG-C Rack component SHALL be the Server Equipment Cabinet

Detailed specifications of this component is provided in Appendix D.

Requirement ID: [SRS-4-167]

All IEG-C components SHALL be rack mounted.

4.9.5 Uninterruptible Power Supply (UPS)

Requirement ID: [SRS-4-168]

The IEG-C UPS component SHALL be the UPS APC Smart-UPS C 1500..

Detailed specifications of this component is provided in Appendix D.

Requirement ID: [SRS-4-220]

The IEG-C power distribution component SHALL be the Powerstrip Conteg.

Detailed specifications of this component is provided in Appendix D.

4.9.6 Cabling

Requirement ID: [SRS-4-169]

The IEG-C components providing 1000BASE-SX gigabit Ethernet physical interfaces SHALL be connected with multi-mode fibre optic cables.

Requirement ID: [SRS-4-172]

All network interfaces shall be implemented in accordance with [IEEE 802.3:2012], whereby, gigabit Ethernet interfaces shall support a maximum transmission unit (MTU) of 9000 bytes.

5 Non-Functional Requirements

5.1 Introduction

This chapter specifies the general non-functional requirements for the IEG-C (Section 5.2) and the specific non-functional requirements for the 'Web Guard Capability' (WG)[2] (Section 5.3) and the 'Mail Guard Capability' (Section 5.4). Depending on the nature of a requirement, requirements that are specified for the IEG-C may apply to the IEG-C as an integrated system of components, or to each of its individual components (including the WG), or to both. The specified components have been selected based on the current IEG-C configuration in NATO theatres. Therefore certain NFRs, e.g. performance efficiency requirements, do not need to be specified for these components.

[2] Note that the abbreviation 'WG' stands for the capability, and not necessarily for a single (physical or virtual) system; in other words, a Web Guard Capability may be composed of more than one system. (See APPENDIX A for a general system description of the WG.)

The Non-Functional Requirements (NFR) categorizes system/software product quality properties into the following characteristics:

- Performance efficiency – Sections 5.2.1 and 5.3.1;
- Compatibility-interoperability – Section 5.2.2;
- Usability – Sections 5.5 and 5.3.2;
- Reliability – Sections 5.2.4 and 5.3.3;
- Security – Sections 5.2.5 and 5.3.4;
- Maintainability – Sections 5.2.6 and 5.3.5;
- Portability – Section 5.2.7 and 5.3.6;
- Survivability – Section 5.2.8 and 5.3.7;
- Environment – Section 5.2.9;
- Equipment (Static) – Section 5.2.10;
- Equipment (DCIS) – Section 5.3.4.2.

Characteristic definitions in this section are based on ISO/IEC 25010:2011(E) - System and software quality models [ISO/IEC 25010, 2011].

5.2 IEG-C Non-Functional Requirements

5.2.1 Performance Efficiency

Description: Performance relative to the amount of resources used under stated conditions.

NOTE Resources can include other software products, the software and hardware configuration of the system, and materials (e.g. print paper, storage media).

5.2.1.1 Time Behaviour

Description: Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.

Requirement ID: [SRS-5-1]

The IEG-C SHALL have all functionality ready to use for an authorised user after invoking the system function within 5 minutes.

Requirement ID: [SRS-5-2]

The IEG-C SHALL execute the log-in function within 30 seconds.

Requirement ID: [SRS-5-300]

The IEG-C SHALL meet at a minimum the throughput levels defined for the individual data types shown Table 6 .

Table 6: IEG Capacity Requirements per Data Type

Data Type	Protocol	Mediator	Size (min- max)	Frequency
Directory (GAL)	LDAP	Firewall only	1KB - 10MB	12x/day
Identity & Access Mgmt	LDAP	Firewall only	<1KB	
Domain Name Services	DNS	Firewall only	<1KB	
Web browsing NS to MS	HTTP/S	Web Proxy	1KB-100MB	
File Transfer (RS)	FTP/HTTP	Web Guard	1KB-100MB	100/Day
File Transfer (other)	FTP/HTTP	Web Proxy	1KB-100MB	100/Day
Full motion video	STANAG 4609	Web Guard	188 byte	25000 /s
Instant Messaging	HTTP/S	Web Guard	<1Kb - 1Mb	1/day - 10/sec
Jchat / XMPP	XML	Web Guard	<1Kb - 1Mb	1/day - 10/sec
Formal Messaging	SMTP	Mail Guard	1KB-1MB	50/Day
Email (informal)	SMTP	Mail Guard	1kb-10Mb	2000/day
Remote Desktop	RDP	RDP Proxy	100KB streaming	5 concurrent sessions
IntelFS	HTTP	Web Guard	1KB-100MB	50/day
COP	Link-16, OTH-G	Web Guard		See air/maritime tracks
Maritime Tracks	OTG	Web Guard	1kb-10Mb	1package/30sec -5Min
Land Force Tracks	FFI/NFFI	Web Guard	<1KB	500 packets / 30 Sec

Data Type	Protocol	Mediator	Size (min- max)	Frequency
Air Tracks	Link-16, JREAP, OTH-Gold	Web Guard	<1Kb	<400 -500 packages/sec
Tactical Data Links	This is officially L16, L1, L11, L22	Web Guard	<1Kb	<400 -500 packages/sec
BMD Tracks	Link-16	DISG/Web Guard		See Air Tracks

Requirement ID: [SRS-5-301]

The IEG-C SHALL meet the minimum required throughput defined in Table 6, for at least 99.5% of its Operational time.

Requirement ID: [SRS-5-302]

The IEG_C services SHALL never drop below the maximum throughput value defined Table 6 by more than 10%.

Requirement ID: [SRS-5-311]

The information contained in Table 6 SHALL be used to define key performance indicators (KPIs) for ‘Availability’, ‘Quality’ and ‘Usage’, as defined in [NCIA SMC TA, 2018].

5.2.1.2 Scalability

The system shall be scalable so that IEG-C capacity can be increased.

Requirement ID: [SRS-5-3]

The IEG-C SHALL be designed to allow future scalability.

Requirement ID: [SRS-5-4]

The IEG-C SHALL be expandable and scalable in performance (throughput and bandwidth).

Requirement ID: [SRS-5-5]

The IEG-C SHALL be capable of accommodating additional functionality the need for which may arise as well as future technological improvements.

Requirement ID: [SRS-5-6]

The IEG-C SHALL use an architecture that allows horizontal scalability and allows the same component to be deployed on multiple machines supporting the information exchange requirements in concert.

Requirement ID: [SRS-5-7]

In order to keep meeting the requirements on Time Behaviour in 5.2.1.1 it SHALL be possible to apply horizontal scalability without disrupting the services offered by the IEG-C.

Requirement ID: [SRS-5-9]

The IEG-C SHALL be Vertical Scalable, i.e. IEG-C SHALL be able to adapt its performance characteristics by adding additional system resources such as processing power, memory, disk capacity, or network capacity.

Requirement ID: [SRS-5-10]

The IEG-C SHALL be able to support additional system resources (introduction of additional storage capacity or server processing power) without having to modify the system architecture, replace existing components, interrupt or degrade current functional and performance requirements.

Requirement ID: [SRS-5-303]

The Platform SHALL be able to support a throughput increase of 10% every year for a period of 5 years with no degradation of the maximum latency.

Requirement ID: [SRS-5-329]

The IEG-C as a system SHALL support the use of multiple instances in parallel, providing same gateway services between identical Low and High domains and being operated in different physical locations.

Requirement ID: [SRS-5-330]

When multiple IEG-C are operated in parallel between identical Low and High domains, it SHALL be possible to identify per information flow, which IEG-C acts as the primary gateway and those which act as alternates.

Requirement ID: [SRS-5-331]

The fall back mechanism SHALL support a seamless transition from the primary IEG-C to an alternate IEG-C for users and system administrators.

Requirement ID: [SRS-5-332]

It SHALL be possible to identify on the monitoring system which IEG-C (primary or alternate) is currently servicing each of the information flows.

Requirement ID: [SRS-5-333]

The IEG-C SHALL be able to operate 72 hours in total isolation from any central management and monitoring system.

5.2.2 Compatibility-Interoperability

5.2.2.1 Interface Requirements

Interoperability is defined in ISO 25010 as the degree to which two or more systems, products or components can exchange information and use the information that has been exchanged. Description: Within NATO, interoperability is defined as, the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.

5.2.2.1.1 Principles of Alliance C3 Interoperability

The following principles are defined in Alliance Consultation Command and Control (C3) Interoperability Policy, 17th February 2015.

Use of an Architectural Approach to provide Coherence

- NATO C3 Interoperability Requirements (C3 IOR) shall be expressed in terms of the required sharing of information and ICT services and shall be identified and consolidated by the NATO Military Authorities (NMA) and Staffs within NATO capability requirement statements for execution by NATO and Nations.
- Architecture products shall serve to inform, guide and document interoperability of C3 Capabilities and ICT Services in their lifecycle.

Identification of Standards and Profiles as the basis for Interoperability Solutions

- Standards and profiles shall be included within the NATO Interoperability Standards and Profiles (NISP).
- NATO Enterprise entities shall ensure the service interface profiles associated with the C3 Capabilities and ICT Services they develop and provide are published in the NISP and are available for verification and validation testing to other NATO Enterprise entities and NATO Nations.
- NATO architectures shall utilise the agreed standards (STANAGs) and profiles from the NISP as appropriate to achieve the required interoperability of C3 Capabilities and ICT Services.
- Appropriate interoperability solutions and procedures to match C3 IOR over time shall be identified/developed and documented by the implementer and coordinated with the C3 Board as appropriate.
- NATO Enterprise entities shall implement and adopt the appropriate interoperability solutions and procedures to meet agreed C3 IOR. This will involve the achievement of semantic as well as syntactic, empirical and physical interoperability.

Verification and validation of Interoperability Solutions through Testing

- Interoperability of solutions to C3 IOR shall be verified and validated by testing regularly during the life cycle, in accordance with the provisions of this policy.
- Testing of the interfaces of C3 Capabilities and ICT Services shall be conducted, including testing against the agreed standards and profiles that are contained within the NISP. Testing at National level is a national responsibility and NATO is responsible for testing as a Host Nation.
- C3 Capabilities and ICT Services shall have their interfaces pass NATO level C3 Interoperability tests; this testing shall be between NATO, NATO Nations

and Partners Nations C3 Capabilities and ICT Services interfaces, based on the NATO agreed standards and profiles that are contained within the NISP. The testing shall include assessment, analysis, evaluation, verification, validation and up to, but not including, the certification of C3 Capabilities and ICT Services.

- The status of interoperability testing of STANAGs is valuable information that must be recorded. To the extent possible, this information shall be included in the NISP.
- A harmonised spectrum of test capabilities shall be established and used to verify and validate NATO and national C3 interoperability. Test activities shall include technology demonstration and experimentation, standards development and implementation, system interoperability testing, field, pre-deployment and reference system testing.

The mandatory standards and profiles documented in the latest version of NISP will be used in the implementation of NATO Common Funded Systems. Participating nations agree to use the mandatory standards and profiles included in the NISP at the Service Interoperability Points and to use Service Interface Profiles among NATO and Nations to support the exchange of information and the use of information services in the NATO realm.

Requirement ID: [SRS-5-11]

The IEG-C SHALL use the existing interoperability profiles and provide any new profiles into the NATO Interoperability Standards and Profiles [ADatP-34] (NISP) volumes after all implementation is completed.

Requirement ID: [SRS-5-12]

The IEG-C software code and components SHALL comply with the latest version of the NATO Interoperability Standards and Profiles (NISP). Any deviation is to be justified and reviewed by the Technical Project Board.

Requirement ID: [SRS-5-13]

The IEG-C SHALL be compliant with NATO document AC/35-D/2002 "Directive on Security of Information".

Requirement ID: [SRS-5-14]

The IEG-C SHALL comply with NATO document "Primary Directive on CIS Security" [AC/35-D/2004-REV3].

Requirement ID: [SRS-5-15]

The IEG-C SHALL be compliant with the NATO document "INFOSEC Technical and Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools (ST)" [AC/322-D(2004)0030].

Requirement ID: [SRS-5-17]

The IEG-C SHALL be compliant with NATO document “Security within the North Atlantic Treaty Organisation” [NAC C-M(2002)49-COR12].

5.2.2.1.2 Information Exchange Requirements

Requirement ID: [SRS-5-18]

The IEG-C SHALL guarantee all incoming and outgoing formatted messages are valid according to the specified formats.

5.2.2.1.3 Security Services

Requirement ID: [SRS-5-19]

The IEG-C primary security services (access control, confidentiality, integrity, authentication, and non-repudiation) SHALL be supported by X.509

Requirement ID: [SRS-5-20]

The IEG-C X.509 support to primary security services SHALL be compliant with NPKI.

5.2.2.2 Handling Country Codes

STANAG 1059 [STANAG 1059] aims to provide unique 3-letter codes to distinguish geographical entities, nations and countries for use within NATO from 01 April 2004. Participating nations agreed to use the codes as defined in Annexes A and B of the STANAG, whenever it is necessary to use abbreviations in publications, documents, orders or other media, to identify geographical entities, nations and countries or any part of national forces.

Requirement ID: [SRS-5-21]

The IEG-C SHALL use country codes according to “Letter Codes for Geographical Entities” [STANAG 1059].

5.2.2.3 Time Synchronization

Requirement ID: [SRS-5-22]

The IEG-C SHALL provide accuracy of timing for messaging time stamps (e.g., time of receipt, send, release authorisation, etc.) to one millisecond. Other system-level functions (e.g., process synchronisation) may require additional accuracy as required for correct operation.

Requirement ID: [SRS-5-23]

The IEG-C SHALL synchronize its internal system clocks with a source on the ON using the Network Time Protocol (NTP).

5.2.3 Usability

5.2.3.1 Compliance with standards and Guide Lines

5.2.3.1.1 NCI Agency and NATO

Bi-SC AIS applications are developed as projects within the NCI Agency (NCIA) to be used by NATO users. Both NCIA and NATO have their own standards and guidelines

that will influence or directly affect Bi-SC AIS applications' visual design. Although Bi-SC AIS applications can have their own identity, any new application needs to feel like other products NCIA or NATO have previously created and share the same organizational values.

Requirement ID: [SRS-5-24]

The visual design of the IEG-C SHOULD follow the recommendations and guidelines stated in the following Documents:

- NATO Visual Identity Guidelines [NATO VIG v3]

5.2.3.1.2 ISO standards

Requirement ID: [SRS-5-25]

The IEG-C icons included in the designed solution SHALL be compliant with the ISO 18152 standard series.

Requirement ID: [SRS-5-26]

The IEG-C SHALL be compliant with the ISO 9241 standard series. In particular:

Requirement ID: [SRS-5-27]

The IEG-C SHALL be compliant to ISO 9241-12 for the presentation of information.

Requirement ID: [SRS-5-28]

The IEG-C SHALL be compliant to ISO 9241-13 for user guidance.

Requirement ID: [SRS-5-29]

The IEG-C SHALL be compliant to ISO 9241-14 for menu dialogues.

Requirement ID: [SRS-5-30]

The IEG-C SHALL be compliant to ISO 9241-16 for direct manipulation dialogues

Requirement ID: [SRS-5-31]

The IEG-C SHALL be compliant to ISO 9241-143 for form filling dialogues

Requirement ID: [SRS-5-32]

The IEG-C SHALL be compliant to ISO 9241-171 for accessibility.

Requirement ID: [SRS-5-33]

The IEG-C SHALL follow the dialogue principles stated in ISO 9241-110.

5.2.3.2 Log-on procedures

Requirement ID: [SRS-5-34]

In applications where users must log-on to the system, log-on SHALL be a separate procedure that must be completed before a user is required to select among any operational options.

Requirement ID: [SRS-5-35]

Appropriate prompts for log-on SHOULD be automatically displayed on the user's terminal when accessing the application.

Requirement ID: [SRS-5-36]

User identification procedures SHALL be as simple as possible, consistent with adequate data protection.

Requirement ID: [SRS-5-37]

When required, the password SHALL not be echoed on the display. An asterisk (*) or similar symbol will be displayed for each character when inputting secure passwords during log-on.

Requirement ID: [SRS-5-38]

Users SHALL be provided feedback relevant to the log-on procedure that indicates the status of the inputs.

Requirement ID: [SRS-5-39]

If a user cannot log-on to a system, a prompt SHOULD be provided to explain the reason for this inability. Log-on processes SHOULD require minimum input from the user consistent with the requirements prohibiting illegal entry.

5.2.3.3 Log-off procedures

Requirement ID: [SRS-5-40]

When a user signals for system log-off, or application exit or shut-down, the system SHOULD check pending transactions to determine if data loss seems probable. If so, the computer SHOULD prompt for confirmation before the log-off command is executed.

5.2.4 Reliability

Description: Degree to which a system, product or component performs specified functions under specified conditions for a specified period of time.

NOTE 1 Adapted from ISO/IEC/IEEE 24765.

NOTE 2 Wear does not occur in software. Limitations in reliability are due to faults in requirements, design and implementation, or due to contextual changes.

NOTE 3 Dependability characteristics include availability and its inherent or external influencing factors, such as availability, reliability (including fault tolerance and recoverability), security (including confidentiality and integrity), maintainability, durability, and maintenance support.

For services, a failure is characterized by the inability of the Service to perform its operation.

For web-based applications, an error requiring the user to reload the browser shall be considered a failure.

Systems that require high reliability should also require high verifiability to make it easier to find defects that could compromise reliability.

For the Monitoring of reliability characteristics, the following definitions will be used:

a. Error (or Fault): A design or source code or hardware flaw or malfunction that causes a Failure of one or more Configuration Items. A mistake made by a person or a faulty Process that affects a CI is also an Error (human Error). For the IEG-C, Human Error is generally not taken into consideration in measuring the quality Performance.

b. Fault: see Error

c. Failure: Loss of ability to Operate to Specification, or to deliver the required output. The term Failure may be used when referring to Services, Processes, Activities, or Configuration Items.

d. Incident: An unplanned interruption to a service or reduction in the quality of a service. Failure of a Configuration Item that has not yet affected service is also an Incident — for example, Failure of one disk from a mirror set

e. Problem: A cause of one or more Incidents. The cause is not usually known at the time the Incident happens.

5.2.4.1 Availability

Description: Degree to which a system, product or component is operational and accessible when required for use.

Inherent Availability (Intrinsic): assumes ideal support (i.e., unlimited spares, no delays, etc.), only design related failures are considered: Ai = MTBF/ (MTBF + MTTD+MTTRSy).

Operational Availability: considers logistics support, A0 = MTBM / (MTBM + MDT).

- MTTD is the Mean Time To Diagnose.
- MTTRSy is the Mean Time To Restore (the System).
- MTBF is the Mean Time Between Failures.
- MTTR is the Mean Time Ro Repair as a function of design.
- MTBM is the Mean Time Between Maintenance, all corrective and preventive maintenance.
- MDT is the Mean Down Time, which includes the actual time to perform maintenance and accounts for any delays in getting the needed personnel, upgrades, installations, parts etc...

Requirement ID: [SRS-5-304]

The IEG-C SHALL exhibit a Mean-Time-Between-Failure (MTBF) characteristic of at least 8760 operational hours.

5.2.4.2 Inherent Availability

Requirement ID: [SRS-5-41]

The IEG-C SHALL be available in operational HQs, static and deployed, 24 hours a day, 7 days a week, with an availability rate of 99.5 %.

5.2.4.3 Operational Availability

Description: Operational Software to be in a state to perform a required function at a given point in time, under stated conditions of use.

Table 5 shows the levels of operational continuity for the desired availability:

Table 7 Levels of Operational Continuity per desired availability percentage

Level	Operational Continuity						Disaster Recovery	
	% Availability	Monthly Unplanned Downtime	Monthly Planned Downtime	Degraded Service	Max Restoration time	Max Allowable Data Loss	Recovery Time	Recovery Point
L1	99.99	<1 hr	<1 hr	None	1 hr	1 hr	N/A	N/A
L2	99.9	1 hrs	6 hrs	Minimal	2 hrs	4 hrs	4 hrs	8 hrs
L3	99	7 hrs	12 hrs	Some	4 hrs	8 hrs	12 hrs	24 hrs
L4	98	14 hrs	36 hrs	Allowed	12 hrs	24 hrs	48 hrs	48 hrs

Requirement ID: [SRS-5-42]

The IEG-C, including hardware, infrastructure and Operational Software, SHALL be available for use at static sites (via Data Centres) 24 hours per day, 365 days per year with an availability of 99.9% (Level 2 of Operational Continuity).

The IEG-C (including hardware, infrastructure and Operational Software) availability does not rely on enabling services external to the IEG-C. Hence, its availability depends solely of the intrinsic availability of the hardware and software elements that make the IEG-C.

Requirement ID: [SRS-5-318]

The IEG-C, as a system, SHALL have an availability of 99.95%.

5.2.4.4 Fault Tolerance

Description: Degree to which a system, product or component operates as intended despite the presence of hardware or software faults.

Requirement ID: [SRS-5-43]

The IEG-C SHALL, despite the presence of hardware or software faults in part of the IEG-C, continue to perform the unaffected IEG-C functions.

Requirement ID: [SRS-5-44]

The IEG-C Servers SHALL gracefully degrade in the condition where any dependent services and components are not available and notify the user of the limited functionality.

Requirement ID: [SRS-5-319]

Upon restoration of services, the IEG-C Servers SHALL become fully operational.

Requirement ID: [SRS-5-46]

The IEG-C SHALL provide a rate of fault occurrence of less than 2 failures for 1000 hours of operation in the IEG-C software components, with 95% confidence. A failure is defined as an error or cessation in the operation of the software requiring, as a minimum, a restart of the software (for example, a service) to recover.

Requirement ID: [SRS-5-47]

It SHALL be possible to correct any individual fault within the IEG-C within a period of time no greater than sixty (60) minutes.

5.2.4.5 Maturity

Description: Degree to which a system, product or component meets needs for reliability under normal operation.

NOTE: The concept of maturity can also be applied to other quality characteristics to indicate the degree to which they meet required needs under normal operation.

Requirement ID: [SRS-5-48]

The IEG-C SHALL exhibit a mean-time-between-failure (MTBF) characteristic of less than 2 failures every 7000 hours, and that SHALL not be affected by the total number of IEG-C instances which are active during that period. The MTBF measurement SHALL not include failures resulting from factors determined to be external to the IEG-C (e.g., loss of domain controller).

5.2.4.6 Recoverability

Description: Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.

NOTE Following a failure, a computer system will sometimes be down for a period of time, the length of which is determined by its recoverability.

Requirement ID: [SRS-5-49]

The IEG-C SHALL support recovery from backup and archive data to a stable (consistent) state with minimal data loss.

Requirement ID: [SRS-5-50]

The IEG-C SHALL provide authorised users with the ability to perform full and/or incremental backups of the system's data and software without impacting system availability.

Requirement ID: [SRS-5-327]

The IEG-C backups SHALL be stored on the domain Disaster Recovery System (DRS) or, if the domain DRS is not available, a removable, local backup device.

Requirement ID: [SRS-5-334]

The IEG-C local backup dedicated hardware SHALL be removable in no more than 5 minutes, SHALL not exceed 5kg in weight and SHALL not exceed 30cmx30cmx30cm (Height, Wide, Deep).

Requirement ID: [SRS-5-51]

The IEG-C SHALL maintain full functionality and performance in the event of power failure(s) for a minimum of twenty (20) minutes, prior to initiating a graceful system shutdown.

Requirement ID: [SRS-5-52]

In case of a failure in the power supply to the IEG-C UPS, the IEG-C SHALL react at 50% battery level with a warning and at 30% battery level with going into graceful system shutdown..

Requirement ID: [SRS-5-53]

After going into graceful system shutdown caused by a power failure, the IEG-C SHALL have retained all the relevant data.

Requirement ID: [SRS-5-54]

The IEG-C SHALL provide automatic resumption of operation after power restoration, except where this violates security requirements.

Requirement ID: [SRS-5-55]

The IEG-C SHALL queue pending asynchronous (i.e. do not need immediate feedback) requests to an unavailable service and deliver them when the service becomes available again.

Requirement ID: [SRS-5-56]

The IEG-C SHALL provide a Mean Time To Repair (MTTR) after the failure of a critical component of four (4) hours or less.

Requirement ID: [SRS-5-57]

The IEG-C SHALL provide a maximum time to restore the service after the failure of a critical component of no greater than six (6) hours at the 95% confidence level.

Requirement ID: [SRS-5-58]

The IEG-C SHALL provide a Time-To-Repair (TTR) of no greater than eight (8) hours for servers and their components at 100% confidence level.

Requirement ID: [SRS-5-59]

In case of IEG-C failure the availability interruption SHALL not exceed two hours.

5.2.4.7 Robustness

Requirement ID: [SRS-5-60]

The IEG-C SHALL resume/retry IEG-C services in case of high latency/timeout/loss of network connectivity without loss of data. High latency is defined as latency exceeding one (1) minute.

Requirement ID: [SRS-5-61]

The IEG-C SHALL provide a Mean Time Between Maintenance (MTBM) for individual components of greater than six thousand (6000) hours of continuous operation where the required maintenance action excludes restart of the hardware and software.

Requirement ID: [SRS-5-62]

The IEG-C SHALL provide a MTBM of greater than thousand (1000) hours of continuous operation where the required maintenance action is only a restart of the hardware or software.

5.2.5 Security

Description: Security is defined as the capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and such that authorised persons or systems are not denied access to them.

As well as data stored in or by a product or system, security also applies to data in transmission.

For purposes of this SRS, the following definitions are used:

- Confidentiality: the property that information is not made available or disclosed to unauthorised individuals or entities.
- Integrity: the property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.
- Non-repudiation: the measure of assurance to the recipient that shows that information was sent by a particular person or organisation and to the sender that shows that information has been received by the intended recipients.
- Accountability: the degree to which actions of an entity can be traced uniquely to the entity.
- Authenticity: the degree to which the identity of a subject or resource can be proved to be the one claimed.

The following INFOSEC functionalities will be provided by the BI-SC AIS:

- Confidentiality. Military-grade NATO IP cryptographic equipment (NICE) will provide confidentiality to User data as well as cryptographic separation between security Domains (for example, NATO SECRET, NATO UNCLASSIFIED. MISSION SECRET). Information exchange between these security domains will be achieved through appropriate boundary protection services (BPS). As a minimum, NICE will be located at each boundary between the local area networks (LANs) and the NATO wide area network (WAN). This will ensure that all User data will be encrypted prior to transmission across the NATO WAN. Software application layer mechanisms will be used for Community-of-Interest (COI) separation.
- Integrity. Digital signatures and authentication services will be used by various protocols (e.g., SNMP, IPSEC) to provide integrity and strong authentication to User data and network configurations. The NATO Public Key Infrastructure (NPKI) will enable these specific security services.

Infrastructure security as provided by the Bi-SC AIS Infrastructure will be transparent to the IEG-C.

Requirement ID: [SRS-5-63]

The IEG-C SHALL comply with security settings, installation guides and configuration guidelines listed in the latest approved version of the NCIA CSSL Security Configuration Catalogue.

Requirement ID: [SRS-5-64]

The IEG-C components SHALL be configured with the latest security patches and updated with the latest security guidelines from the NATO Information Assurance Technical Centre (NIATC).

Requirement ID: [SRS-5-65]

The IEG-C SHALL be capable of operating within the NS and MS WAN environment (including servers, network, services and workstations) in the presence of the currently approved NATO Security Settings (target version to be provided by the Purchaser during the Design Stage). Any deviations from the approved security settings SHALL be identified by the Contractor prior to testing and SHALL be subject to approval of the Purchaser.

5.2.5.1 Authenticity

5.2.5.1.1 General

Definitions:

- User: refers to a person having access to the operating system (an OS User) and IEG-C Services. Each User of the IEG-C is assigned Access Rights based on its Role, the Permissions within that Role, and optionally the organization of the User.
- Role: Defined by a set of permissions (i.e., access to objects and functionality) to perform certain operations.

The primary roles in the IEG-C are those defined in Section 3.4.6: System Administrator, Audit Administrator, CIS Security Administrator, Cyber Defence Administrator, and SMC Administrator.

Where in the requirements that follow the general term “IEG-C Administrator” is used to denote one of the primary roles, the reader shall substitute the general term for the applicable primary role based on the requirement.

5.2.5.1.2 Authentication Processing

Requirement ID: [SRS-5-66]

The IEG-C SHALL uniquely Identify and Authenticate Users.

Requirement ID: [SRS-5-67]

The IEG-C SHALL allow an IEG-C Administrator to manage (create, update, delete) IEG-C User Accounts, password details, and assign User Roles to User Account and manage general access privileges of individual User Accounts.

Requirement ID: [SRS-5-68]

The IEG-C SHALL support the application of a password policy.

Requirement ID: [SRS-5-69]

The IEG-C SHALL be configurable to deny the re-use of a specified previous passwords.

Requirement ID: [SRS-5-70]

IEG-C SHALL be configurable to lock user accounts after a specified number of unsuccessful authentication attempts.

Requirement ID: [SRS-5-71]

IEG-C passwords SHALL be stored in encrypted form.

Requirement ID: [SRS-5-72]

IEG-C SHALL support the locking of accounts that are no longer required for a specified period of time after which they SHALL be deleted.

Requirement ID: [SRS-5-73]

The IEG-C SHALL support the protection of User credentials in transit.

Requirement ID: [SRS-5-74]

The IEG-C SHALL provide privileged IEG-C accounts (e.g., system and security administrator accounts).

Requirement ID: [SRS-5-75]

The IEG-C SHALL allow authenticated Users to manage their password.

Requirement ID: [SRS-5-305]

The IEG-C SHALL implement Identity and Access Management (IAM) according to the requirements on IAM as specified in the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-5-306]

In support of the authentication and authorization of users, the IEG-C and its sub-components SHALL support authentication and authorization based on the RADIUS protocol [IETF RFC 2865, 2000].

Requirement ID: [SRS-5-308]

The IEG-C SHALL implement multifactor user authentication in accordance with in the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].

Requirement ID: [SRS-5-309]

The implementation of multifactor authentication by the IEG-C SHALL integrate with the multifactor authentication solution as it is in use in the NATO Enterprise.

5.2.5.2 Audit and Accountability

Requirement ID: [SRS-5-76]

The IEG-C SHALL generate audit records for auditable events, addressing, among others, the following events:

- system start-up (including re-starts) and shutdown;
- log-on (including log-on attempts) and log-off of individual users
- changes to permissions and privileges of users and groups;
- changes to security relevant system management information(including audit functions);
- start-up and shutdown of the audit function;
- any access to security data;
- deletion, creation or alteration of the security audit records;
- changes to system date and time;
- unsuccessful attempts to access system resources;

Requirement ID: [SRS-5-77]

Audit tracing in the IEG-C SHALL be permanently effective.

Requirement ID: [SRS-5-78]

The IEG-C SHALL protect the information from unauthorised modification or deletion.

Requirement ID: [SRS-5-79]

The IEG-C SHALL establish access permissions to audit information.

Requirement ID: [SRS-5-80]

The IEG-C SHALL associate individual user identities to auditable events in the event log.

Requirement ID: [SRS-5-81]

The IEG-C SHALL include the date and time of each auditable event in the event log.

Requirement ID: [SRS-5-82]

The IEG-C SHALL alert an IEG-C Administrator on failed attempts at log-on.

Requirement ID: [SRS-5-83]

The IEG-C SHALL create and maintain an archive of audit information.

Requirement ID: [SRS-5-84]

The IEG-C SHALL support the retaining of audit information for a specified period of time.

5.2.5.2.1 User Audit Log

Requirement ID: [SRS-5-85]

The IEG-C SHALL record in traceable logs all selected transactions, database activities, technical events (e.g., dataset synchronisation, directory replication) and accessing of data.

Requirement ID: [SRS-5-86]

If so configured, the IEG-C SHALL log all configurations changes with the trace to persons or systems.

5.2.5.2.2 System Audit Log

Requirement ID: [SRS-5-87]

The IEG-C SHALL generate and maintain an Audit Log for each of the following auditable events, SHALL associate individual User identities to those events, and SHALL include date and time of the event, type of event, User identity, and the outcome (success or failure) of the event:

- System start-up and shutdown,
- the start/end time of usage of system applications (system components) by individual Users

- Changes to permissions and privileges of Users and groups,
- Changes to security relevant system management function,
- Configuration changes,
- Any access to audit log,
- Deletion, creation or alteration of the security audit records,
- All privileged operations,
- All updates of IEG-C access rights,
- All attempts to delete, write or append the Audit files.

Requirement ID: [SRS-5-88]

The IEG-C SHALL use integrity checking countermeasures to ensure that the Audit Log has been archived successfully.

Requirement ID: [SRS-5-89]

The IEG-C SHALL support the following warning system events based on configurable limits:

- Network bandwidth low;
- Percentage of disk space left;
- Percentage of table space left.

5.2.5.3 Application Security

5.2.5.3.1 Session Management

Requirement ID: [SRS-5-90]

Sessions SHALL be invalidated when the user logs out.

Requirement ID: [SRS-5-91]

Sessions SHALL timeout after a specified period of inactivity.

5.2.5.3.2 Input validation

Requirement ID: [SRS-5-92]

The runtime environment or parser SHALL not be susceptible to XML and XPath injection.

Requirement ID: [SRS-5-93]

The IEG-C SHALL have defences against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)

5.2.5.3.3 Data Protection

Requirement ID: [SRS-5-94]

Sensitive data SHALL be sanitized from memory as soon as it is no longer needed.

5.2.5.3.4 Communications Security

Requirement ID: [SRS-5-95]

A certificate path SHALL be built and validated from a trusted CA to each Transport Layer Security (TLS) server certificate, and each server certificate SHALL match the Fully Qualified Domain Name of the server.

Requirement ID: [SRS-5-96]

Failed TLS connections SHALL not fall back to an insecure connection.

Requirement ID: [SRS-5-97]

Certificate paths SHALL be built and validated for all client certificates using configured trust anchors and revocation information.

5.2.5.3.5 Business Logic

Requirement ID: [SRS-5-98]

The application logic SHALL have protection mechanisms against application crashing, memory access violations (buffer overflow) and unexpected exceptions such as data destruction and resource depletion (Memory, CPU, Bandwidth, Disk Space, etc.).

Requirement ID: [SRS-5-99]

The application SHALL have sufficient access controls to prevent elevation of privilege attacks.

5.2.6 Maintainability

Description: Degree of effectiveness and efficiency with which a product or system can be modified by the intended maintainers

NOTE 1 Modifications can include corrections, improvements or adaptation of the software to changes in environment, and in requirements and functional specifications. Modifications include those carried out by specialized support staff, and those carried out by business or operational staff, or end users.

NOTE 2 Maintainability includes installation of updates and upgrades.

NOTE 3 Maintainability can be interpreted as either an inherent capability of the product or system to facilitate maintenance activities, or the quality in use experienced by the maintainers for the goal of maintaining the product or system.

5.2.6.1 Modularity

Description: Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components.

The system should be composed of discrete components such that a change to one component has minimal impact on other components.

Requirement ID: [SRS-5-100]

The IEG-C SHALL be composed of discrete components such that a change to one component has minimal impact on other components.

Requirement ID: [SRS-5-166]

Any IEG-C component SHALL not exceed 2U height. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.

Requirement ID: [SRS-5-320]

Any IEG-C component SHALL not exceed 20kg. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.

Requirement ID: [SRS-5-321]

Any IEG-C component using forced airflow (fan) cooling SHALL be of front-rear type.

Requirement ID: [SRS-5-322]

All IEG-C component SHALL have dual power supply module. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.

5.2.6.2 Manageability

The system should facilitate efficient and effective management of its operations.

Requirement ID: [SRS-5-101]

The IEG-C SHALL be able to report its status (healthy, warnings, errors) and 'capacity' related aspects for the [IT] resources used (disk, memory, CPU, network) and the application aspects addressed (load, transactions, users) to the NATO EMS environment (in addition to any project specific requirements).

Requirement ID: [SRS-5-102]

The IEG-C SHALL ensure that the application provides management of Personal Information (e.g., User profile and expertise information) held within the IEG-C.

5.2.6.3 Supportability

The system should be easy to support by support personnel.

Requirement ID: [SRS-5-103]

The IEG-C SHALL support remote configuration of all IEG-C components and updates using Microsoft System Center Configuration Manager (SCOM) if available on the platform.

Requirement ID: [SRS-5-104]

IEG-C software assets (including different versions) SHALL have a unique SWID tag assigned.

Requirement ID: [SRS-5-105]

The IEG-C SHALL support collection and reporting of asset inventory metrics for all IEG-C components using Microsoft System Centre Configuration Manager, unless an IEG-C component does not support SCOM, including:

- Memory
- Operating System
- Peripherals
- Services
- Login tracking
- Software existence and usage
- Licensing

5.2.7 Portability

Description: Portability is defined as the capability of the software product to be transferred from one environment to another.

5.2.7.1 Adaptability

Description: Degree to which a product or system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.

Requirement ID: [SRS-5-106]

The IEG-C SHALL be effective and efficient in the adaptation for different or evolving hardware, software or other operational or usage environments.

Requirement ID: [SRS-5-107]

The IEG-C architecture SHALL be designed to permit upgrading for use of new communication, processing and storage technologies during its operational lifetime.

5.2.7.2 Installability

Description: Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.

Requirement ID: [SRS-5-108]

The IEG-C SHALL be equipped with an Installation Guide.

Requirement ID: [SRS-5-109]

The IEG-C Installation Guide SHALL explain all actions to take in order to install and configure the IEG-C, including COTS components. Every action SHALL be followed by a description (text and/or screenshots) of the feedback which will be displayed.

Requirement ID: [SRS-5-110]

The IEG-C Installation Guide SHALL describe:

- Prerequisites for installing the IEG-C. (e.g., the necessary OS access right to be able to install the IEG-C)
- The necessary software, drivers, etc. to install the IEG-C
- How to address integration in the 'environment' (node) - like configuration of monitoring and backup functions
- The (environment specific) configuration changes necessary on the system and the environment
- The required disc space.

Requirement ID: [SRS-5-111]

The IEG-C Installation Guide SHALL describe how to configure the system backbone to be able to run the IEG-C.

Requirement ID: [SRS-5-112]

The IEG-C Installation Guide SHALL contain a description of all configuration files. The following points SHALL be described:

- The location of the configuration file
- The content of the configuration file
- The available settings of the items in the configuration file and their meaning
- How to change the configuration file

Requirement ID: [SRS-5-113]

Two copies of the SWID tag file SHALL be installed on each system that the IEG-C software is installed on. The first copy of the tag file SHALL be accessible in the top level directory of the installed software package itself and the second copy of the tag file SHALL be installed in a platform dependent file system location as:

<file system location>\regid.1997-08.int.nato\<tagfilename>."

Requirement ID: [SRS-5-114]

The IEG-C SHALL provide a capability to completely uninstall IEG-C application(s)/component(s). The IEG-C uninstallation capability SHALL remove all program files and folders, registry entries, program and group folders, as appropriate, retaining all shared and system files.

Requirement ID: [SRS-5-115]

The IEG-C uninstallation capability SHALL not adversely impact other installed applications.

Requirement ID: [SRS-5-116]

The IEG-C SHALL store IEG-C temporary files only in the IEG-C's temporary folders in configurable locations.

Requirement ID: [SRS-5-117]

An IEG-C System Administrator SHALL be able to successfully deploy (i.e., install and configure) a component in the IEG-C within a time frame of one (1) working day after receiving a maximum of five (5) days of training per component.

For Deployable CIS (DCIS), systems and composing modules are being re-configured from scratch each time there is a new mission. To this purpose, an automation and orchestration solution is being used. This tool uses blueprints using API and scripts to connect to elements over different types of interfaces (iLO ports, serial ports, SSH, RESTful, ...) to configure these step-by-step.

Requirement ID: [SRS-5-323]

The IEG-C SHALL be configurable from scratch using the DCIS orchestration and automation toolset.

Requirement ID: [SRS-5-324]

The IEG-C SHALL include an NSAB/NOS endorsed quick erase feature allowing the complete erasure of all configuration, stored data and software.

Requirement ID: [SRS-5-325]

The quick erase feature SHALL not take longer than 30 minutes.

Requirement ID: [SRS-5-326]

The quick erase feature SHALL not erase IEG-C backups.

5.2.7.3 Internationalisation

Requirement ID: [SRS-5-118]

All software and documentation to be provided by the Contractor under this project SHALL be in English (US) version.

5.2.8 Survivability

Requirement ID: [SRS-5-119]

The IEG-C SHALL automatically detect the availability and re-establishment of network connectivity and SHALL initiate subsequent tasks as though network connectivity had not been lost.

5.2.9 Environment

Requirement ID: [SRS-5-121]

The IEG-C SHALL support the use of IPv6 without impaired functionality and performance within a network environment.

Requirement ID: [SRS-5-122]

The IEG-C SHALL be compliant to the requirements specified in this SRS in a virtualized server environment (virtual servers).

5.2.10 Equipment

Requirement ID: [SRS-5-123]

The IEG-C equipment SHALL NOT be damaged nor suffer loss of data, when any of the ambient temperature and humidity conditions contravene operating limits while power is available.

Requirement ID: [SRS-5-124]

The IEG-C support staff SHALL be able to manually resume normal operation of the IEG-C equipment within five (5) minutes from when ambient temperature and humidity conditions return to within operating limits.

5.3 Web Guard Non-Functional Requirements

This section details the additional, Web Guard specific, non-functional requirements, over and above those specified in section 5.2.

5.3.1 Performance Efficiency

5.3.1.1 Capacity

Description: Degree to which the maximum limits of a product or system parameter meet requirements.

NOTE Parameters can include the number of items that can be stored, the number of concurrent users, the communication bandwidth, throughput of transactions, and size of database.

Requirement ID: [SRS-5-125]

The WG SHALL support the concurrent processing of low-to-high and high-to-low traffic and meet the performance objectives for both traffic flows.

Requirement ID: [SRS-5-126]

The WG SHALL support the concurrent execution of low-to-high and high-to-low policy enforcement and meet the performance objectives for each.

Requirement ID: [SRS-5-127]

The WG SHALL support the concurrent execution of all functionality offered by the building blocks Data Exchange Services, Protection Policy Enforcement Services, Protection Services and Element Management Services.

Requirement ID: [SRS-5-128]

On interface WG_IF_NET_HIGH (see 6.4.1.2) the WG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-129]

On interface WG_IF_NET_LOW (see 6.4.1.3) the WG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-131]

The WG SHALL allow an IEG-C System Administrator to perform system management functions regardless of the load on the WG.

Requirement ID: [SRS-5-132]

The WG SHALL support the information exchange of HTTP messages with body size up to ten (10) GB.

Requirement ID: [SRS-5-133]

The WG SHALL support parallel processing of HTTP messages, i.e. it SHALL be possible for the WG to subject multiple different HTTP messages to policy enforcement at the same time.

5.3.1.2 Time Behaviour

Description: Degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements.

5.3.1.2.1 Definitions

Processing time

Let the *'WG processing of an HTTP message'* (or simply *'HTTP message processing'*) be the following sequence:

For a given HTTP message *H*:

- Subject *H* to policy enforcement; and
- If *H* violates the WG security policy: generate (but not send) the appropriate HTTP error message.

Let the *'WG processing time of an HTTP message'* or simply *'HTTP message processing time'* (notation: *T_WG_Proc*) be the time measured in order for the WG to complete the sequence *'HTTP message processing'* above.

When it is written that the *'WG processes an HTTP message'*, this means the same as subjecting an HTTP message to *'HTTP message processing'*. Therefore, the time it takes for the WG to process an HTTP message is equal to T_WG_Proc.

Let the *'WG processing times'* be the processing times that the WG is able to offer.

Throughput

Let the *'WG throughput'*, or simply *'throughput'* be the number of HTTP messages that the WG can process per given time period.

Forwarding time

Let the *'WG forwarding time of an HTTP message'* or simply *'HTTP message forwarding time'* (notation: *T_WG_Forward*) be the time measured in order for the WG to complete the following sequence:

For a given HTTP message *H*:

- Receive *H* at WG_IF_NET_HIGH or WG_IF_NET_LOW;
- If necessary queue *H*; and then
- Execute *'HTTP message processing'* for *H*;
- Then, if *H* did not violate the WG security policy:
    - If necessary queue *H*; and then
    - Forward *H* onto the low domain or high domain respectively.
- Else, if *H* did violate the WG policy:
    - If necessary queue the associated HTTP error message; and then
    - Forward the HTTP error message onto the high domain or low domain respectively.

When it is written that the *'WG forwards an HTTP message'*, this means the same as completing the sequence above.

The *'HTTP message forwarding time'* is equal to the *'HTTP message processing time'* plus the time it takes to receive, queue and forward HTTP messages. (The 'HTTP message forwarding time' is similar to the concept of 'response time' (i.e. 'processing time' + 'queueing time').)

Let the *'WG forwarding times'* be the forwarding times that the WG is able to offer.

5.3.1.2.2 Message size categories

Throughput, processing time and forwarding time depend on message size. Therefore this SRS distinguishes a number of message size categories for the WG.

Let the following terminology denote size categories for HTTP messages. The size categories are determined by the size of the HTTP body.

- Very small HTTP messages: *0 <= HTTP body size <= 150 KB;*
- Small HTTP messages: *150 KB < HTTP body size <= 10 MB;*
- Medium HTTP messages: *10 MB < HTTP body size <= 50 MB;*
- Large HTTP message: *50 MB < HTTP body size <= 100 MB;*
- Very large HTTP messages: *100 MB < HTTP body size <= 10 GB.*

The size categories are based on HTTP body size because that is the part of the HTTP message that is determined by the message size of the product that is being exchanged by the Web Guard between the low and high domain.

5.3.1.2.3 'Normal load' and 'peak load'

Normal load

In this SRS the *'normal load'* is the load on the WG (in terms of HTTP messages to be forwarded) that can be assumed to exist under normal traffic conditions. This SRS defines a *'normal load'* for each size category from 5.3.1.2.2, which is referred to as the *'size category normal load'* (*SCNL*). Then, the 'total normal load' (notation *TNL*) is the sum of all size category normal loads that the WG can be subjected to simultaneously.

The following *'load characteristics'* are distinguished in order to characterize the traffic that comprises the normal load (note that not all load characteristics have to apply to a normal load simultaneously):

- *Average message size;*
- *Maximum message size;* (For the size category *normal load* this is bound by the maximum message size in the category. For the *TNL* this is bound by the maximum message size of the 'very large HTTP messages' category.)
- *Number of messages per time unit;*
- *Message size distribution;*
- *Message type distribution.*

When it is written that the WG 'supports a normal load', this means that the *WG throughput*, the *WG processing times* and the *WG forwarding times* are such that the WG is able to support a continuous normal load without degradation in performance.

Peak load

Let *'peak load'* be a multiple of the normal load (in terms of its load characteristics), during a limited period of time.

5.3.1.2.4 Requirements for WG forwarding times, throughput and processing times

Requirement [SRS-5-134] below specifies the requirements for supporting the normal load per message size category.

Requirement ID: [SRS-5-134]

The WG SHALL support[3] the following normal loads per message size category:

[3] When it is written that the WG 'supports a normal load', this means that the WG throughput*, the* WG processing times *and the* WG forwarding times *are such that the WG is able to support a continuous normal load without degradation in performance.*

- Very small HTTP messages: a *SCNL* of 35000 HTTP messages per minute with average message size 15 KB.
- Small HTTP messages: a *SCNL* of 180 HTTP messages per minute with average message size 5 MB.
- Medium HTTP messages: a *SCNL* of 30 HTTP messages per minute with average message size 30 MB.
- Large HTTP messages: a *SCNL* of 10 HTTP messages per minute with average message size 70 MB.
- Very large HTTP messages: a *SCNL* of 2 HTTP messages per minute with average message size 300 MB.

Requirement ID: [SRS-5-135]

The WG SHALL meet the requirements in [SRS-5-133] under a total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 7 MB;
- *TNL* maximum message size <= 10 GB;
- *TNL* message size distribution: 80% of *TNL* < 150 KB; 95% of *TNL* < 30 MB; 98% of *TNL* < 300 MB.

Requirement ID: [SRS-5-136]

Per size category the average *HTTP message processing time T_WG_Proc-Average* SHALL meet the following constraints under the size category normal loads from [SRS-5-133]:

- Very small HTTP messages: *T_WG_Proc-Average* < 200 milliseconds;
- Small HTTP messages: *T_WG_Proc-Average* < 3000 milliseconds;
- Medium HTTP messages: *T_WG_Proc-Average* < 15000 milliseconds;
- Large HTTP messages: *T_WG_Proc-Average* < 60000 milliseconds;
- Very large HTTP messages: *T_WG_Proc-Average* < 240000 milliseconds.

Requirement ID: [SRS-5-137]

The WG SHALL meet the requirements on *HTTP message processing time* in [SRS-5-135] under a total normal load *TNL* with the following constraints on the *TNL* characteristics:

- *TNL* average message size < 7 MB;
- *TNL* maximum message size <= 10 GB;
- *TNL* message size distribution: 80% of *TNL* < 150 KB; 95% of *TNL* < 30 MB; 98% of *TNL* < 300 MB.

Requirement ID: [SRS-5-138]

If an HTTP message *H* is processed by the WG that is too large for the category 'Very large HTTP messages', the WG SHALL:

- continue to operate;
- be responsive to commands issued by a System Administrator;
- meet the requirements in [SRS-5-133] under the total normal load *TNL*;
- and MAY terminate the processing of *H* in order to do so.

5.3.1.2.5 Requirements for peak load

The following 3 requirements specify the extent to which a peak load may impact the WG throughput, processing times or forwarding times. The peak loads are based on the normal loads from requirement [SRS-5-133]. Each requirement is followed by a rationale.

Requirement ID: [SRS-5-139]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *WG throughput* for that size category SHALL meet the following constraints for the peak load stated, while not rejecting HTTP traffic:

- Very small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.

- Small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Medium HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.
- Very large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, the average *throughput* SHALL decrease at most 10% when compared to the *SCNL*.

Rationale behind [SRS-5-138]: A peak load may require the WG to divert part of its resources to peak load handling, e.g. managing messages queues, potentially affecting resources dedicated to throughput. This requirement aims to limit the impact of a peak load on the WG's throughput. (Because of the temporary nature of a peak load, it may be possible to temporarily make additional system resources available to handle the overhead introduced by the peak load.)

Requirement ID: [SRS-5-140]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *HTTP message forwarding time T_WG_Forward-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting HTTP traffic:

- Very small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 10% when compared to the *SCNL*.
- Small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 20% when compared to the *SCNL*.
- Medium HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 30% when compared to the *SCNL*.'
- Large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 40% when compared to the *SCNL*.
- Very large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Forward-Average* SHALL increase at most 50% when compared to the *SCNL*.

Rationale behind [SRS-5-139]: A peak load implies message queues and hence an increase in forwarding time. This requirements aims to limit the impact on the forwarding

times. (Because of the temporary nature of a peak load, it may be possible to temporarily make resources available to increase throughput such that an increase in forwarding time can be limited.)

Requirement ID: [SRS-5-141]

If, while under the total normal load *TNL*, a peak load occurs for one of the size categories, the average *HTTP message processing time T_WG_Proc-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting HTTP traffic:

- Very small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 5% compared to normal load.
- Small HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 10% compared to normal load.
- Medium HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 20% compared to normal load.
- Large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 30% compared to normal load.
- Very large HTTP messages: for a peak load of 2 times the number of messages in the *SCNL* with a duration of 300 seconds, *T_WG_Proc-Average* SHALL increase at most 40% compared to normal load.

Rationale behind [SRS-5-140]: While under peak load it may not be acceptable for certain types of information exchange, e.g. ‘near real time’ messaging, to have the processing time increased. While for requirements [SRS-5-138] and [SRS-5-139] it is possible to meet those requirements at the cost of processing time (e.g. the number of message processing threads may be increased such that throughput is maintained however per message thread the processing time drops), this requirement aims to limit the increase of the processing times while under peak load.

Requirement ID: [SRS-5-142]

During peak loads that are larger in size or longer in duration than those specified in [SRS-5-138] , [SRS-5-139] and [SRS-5-140] , the WG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject HTTP traffic in order to do so.

Requirement ID: [SRS-5-143]

If peak loads for multiple size categories take place simultaneously, the WG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject HTTP traffic in order to do so.

Requirement ID: [SRS-5-144]

It SHALL be possible to configure an upper size limit, L, such that the WG SHALL reject messages that exceed L.

5.3.1.2.6 Requirements on impact of logging

Requirement ID: [SRS-5-145]

The impact of logging by the WG on its performance SHALL remain within the following limits, for the following log severity levels [RFC 5424]:

- For severity levels ‘Emergency’ (0), ‘Alert’ (1), ‘Critical’ (2), ‘Error’ (3), ‘Warning’ (4): no impact on performance;
- For severity levels ‘Notice’ (5) and ‘Informational’ (6): a decrease in throughput of at most 40%.
- For severity level ‘Debug’ (7): a decrease in throughput of at most 80%.

5.3.1.3 Scalability

Requirement ID: [SRS-5-146]

The WG SHALL be scalable such that when an increase in traffic occurs, capacity can be increased in order to keep meeting the requirements on Time Behaviour in 5.3.1.2.

Requirement ID: [SRS-5-147]

The WG architecture SHALL support horizontal scalability and allow for multiple instances of the WG to be deployed on multiple machines, supporting the information exchange requirements in concert.

Requirement ID: [SRS-5-148]

The WG SHALL be vertically scalable, i.e. the WG SHALL be able to adapt its performance characteristics by having additional system resources added such as processing power, memory, disk capacity, or network capacity.

Requirement ID: [SRS-5-149]

In order to keep meeting the requirements on Time Behaviour in 5.3.1.2 it SHALL be possible to apply horizontal scalability without disrupting the services offered by any active WG.

Requirement ID: [SRS-5-150]

The horizontal scaling of the WG SHALL NOT introduce any additional WG management overhead.

Requirement ID: [SRS-5-151]

The WG SHALL be dimensioned and configured to be able to scale in performance and support the following per a year for three years without degradation of performance as specified in section 5.3.1.2:

- a 200% increase in the *SCNL* (normal load for each HTTP message size category);
- a 50% increase in message size.

5.3.2 Usability

5.3.2.1 Usability

Description: Extent to which an interactive system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

Requirement ID: [SRS-5-152]

The WG SHALL have a high degree of learnability, making it very easy to use for System Administrators even the first time.

Requirement ID: [SRS-5-153]

The WG SHALL score above 80% in user success rate without external support, for System Administrators that have received standard training.

5.3.3 Security

5.3.3.1 Audit and Accountability

5.3.3.1.1 Log Configuration

Requirement ID: [SRS-5-156]

The WG SHALL notify a System Administrator by e-mail when the audit log reaches 75% of its maximum permitted size.

Requirement ID: [SRS-5-310]

The WG System Administrator address SHALL be configurable.

Requirement ID: [SRS-5-157]

The WG SHALL provide a configuration option to set the maximum permitted size of the audit log.

5.3.3.2 Integrity

Requirement ID: [SRS-5-158]

The WG SHALL contain residual information protection mechanisms to ensure that purged information is no longer accessible.

Requirement ID: [SRS-5-159]

The WG SHALL ensure that newly created objects do not contain information that should not be accessible (i.e. information that has been logically deleted).

5.3.4 Maintainability

5.3.4.1 Analysability

Description: Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

NOTE Implementation can include providing mechanisms for the product or system to analyse its own faults and provide reports prior to a failure or other event.

The system shall be effective and efficient in the possibility to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.

Requirement ID: [SRS-5-161]

WG log messages SHALL contain initiating module information, Date/Time (Z), system instance, (log) message, category/severity, user (invoker of function), and context information (like mission/session, service/function, parameters, and trace-log).

5.3.5 Portability

Description: Portability is defined as the capability of the software product to be transferred from one environment to another.

5.3.5.1 Installability

Description: Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.

Requirement ID: [SRS-5-162]

A WG System Administrator SHALL be able to successfully deploy (i.e., install and configure) the WG within a time frame of one (1) working days after receiving a maximum of five (5) days of training.

5.4 Mail Guard Non Functional Requirements

5.4.1 Performance Efficiency

5.4.1.1 Capacity

The degree to which the maximum limits of a product or system parameter meet requirements.

NOTE Parameters can include the number of items that can be stored, the number of concurrent users, the communication bandwidth, throughput of transactions, and size of database.

Requirement ID: [SRS-5-208]

The MG SHALL support the concurrent processing of low-to-high and high-to-low traffic and meet the performance objectives for both traffic flows.

Requirement ID: [SRS-5-209]

The MG SHALL support the concurrent execution of low-to-high and high-to-low policy enforcement and meet the performance objectives for each.

Requirement ID: [SRS-5-210]

The MG SHALL support the concurrent execution of all functionality offered by the building blocks Data Exchange Services, Protection Policy Enforcement Services, Protection Services and Element Management Services.

Requirement ID: [SRS-5-211]

On interface MG_IF_NET_HIGH (see section 7.1.2) the MG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-212]

On interface MG_IF_NET_LOW (see section 7.1.2) the MG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.

Requirement ID: [SRS-5-213]

The MG SHALL queue SMTP messages in the event that policy enforcement functionality is unavailable.

Requirement ID: [SRS-5-214]

The MG SHALL allow an IEG-C System Administrator to perform system management functions regardless of the load on the MG.

Requirement ID: [SRS-5-215]

The MG SHALL support the information exchange of SMTP messages with body size up to ten (10) MB.

Requirement ID: [SRS-5-216]

The MG SHALL support parallel processing of SMTP messages, i.e. it SHALL be possible for the MG to subject multiple different SMTP messages to policy enforcement at the same time.

5.4.1.2 Time Behaviour

The degree to which the response and processing times and throughput rates of a product or system, when performing its functions, meet requirements**.**

5.4.1.2.1 Definitions

Processing time

Let the '*MG processing of an SMTP message*' (or simply '*SMTP message processing*') be the following sequence: